**Executive Summary**

The Group consists of Staying Put which is the parent body and Solace Housing Association ("Solace") which is its subsidiary. Solace Housing Association has adopted a large proportion of the Staying Put Group policies and procedures with the aim of ensuring it is compliant with the regulatory standards. Where existing Group controls are felt to be noncompliant with RSH requirements, the subsidiary has created its own policies, which will supersede those of the Group. In such cases the Group will aim in future to apply Solace HA's policies across the Group to ensure that the highest standards are maintained.

Policies and procedures are in the process of being reviewed, with a number of new policies being created specifically for Solace HA. For those areas where Solace HA will aim to follow the Group structure, it is imperative that the Group ensures these are of the standards required for RPs.

## PART ONE – POLICY STATEMENT

Staying Put recognises the duty of confidentiality owed to those accessing our services, staff and volunteers, as well as the partners we work with, regarding all the ways in which it processes, stores, shares and disposes of information.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified.

The lawful and correct treatment of personal information is very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly. To this end we fully endorse and adhere to the principles of the Data Protection Act 2018 (DPA 18) and General Data Protection Regulation (GDPR).

The Act prohibits the transfer of data outside the UK to countries that do not have similar protection of data except in some circumstances or with the subject's consent.

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our client and human resources function. It also covers our response to any data breach and other rights under the GDPR.

The DPA 18 describes how organisations, including Staying Put must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that all personal data is:

- Processed fairly, lawfully and in a transparent manner;

- Be obtained only for specific, lawful purposes and not in a manner that is incompatible with those purposes;
- Be adequate, relevant and limited to what is necessary for the purpose of processing;
- Be accurate and kept up to date;
- Not be held for any longer than necessary;
- Processed in accordance with the rights of data subjects;
- Be protected in appropriate ways by using appropriate technical and organisational measures;
- Complies with the relevant GDPR procedure for international transferring of personal data if required.

We are committed to following these principles and will process data about you only so far as is necessary for the purpose of managing our business. Data will not be disclosed to anyone else other than our authorised employees, agents, contractors or advisors (except as required by law) unless you expressly authorise its disclosure.

This policy applies to the personal data of all clients, job applicants, existing and former employees, volunteers, workers and self-employed contractors. These are referred to in this policy as relevant individuals and it describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law. We will only process personal data when we have a clear and fair legal basis, and we are transparent about the processing (unless an exemption to transparency applies);

The Staying Put Data Protection Officer who advises on and monitors compliance is: Anita Pluckwell, Head of Operations & Client Care, email: anita@stayingput.org.uk

The Caldicott Guardian who ensures that Staying Put meets the highest ethical and legal standards for processing service user confidential information is: Yasmin Khan, Chief Executive Officer, email: yasmin@stayingput.org.uk

**AIMS AND PRINCIPLES**

- To protect Staying Put from real data security risks including: beaches of confidentiality, failing to offer choice and reputational damage
- To ensure that all staff understand their obligations with regard to any information they come into contact within the course of their work
- To provide assurance to anyone in contact with our service that we have in place the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively
- To safeguard the rights of service users and staff to access any information which is held about them
- To ensure that the records created and held by Staying Put (including electronic records) will be well maintained, protected and appropriately stored and disposed
- To assist, when required, in the safe sharing of information with our clients and partner agencies

## PART TWO – PROCEDURAL GUIDANCE

### 1. Responsibilities

Everyone who works for or with Staying Put has responsibility for ensuring data is collected, stored and handled appropriately. Staff that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Board of Trustees is ultimately responsible for ensuring that Staying Put meets its legal obligations.

The Caldicott Guardians is responsible for:

- Keeping the board updated about data protection responsibilities and risks
- Providing leadership and advice on complex matters involving the use and sharing of service user confidential information, especially in situations where there may be areas of legal and/or ethical ambiguity.
- Promoting the Caldicott Principles and good information governance throughout their organisation, ensuring that information sharing is safe and effective.

The Data Protection Officer is responsible for:

- Reviewing the data protection procedure and related policies, in line with agreed schedule Handling data protection questions from staff and those covered by the policy
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The Executive Assistant is responsible for:

- Processing requests from individuals to see the data Staying Put holds about them (also called subject access requests)

The IT and Health and Safety Lead is responsible for:

- Ensuring all systems, services and equipment used for storing data meet the acceptable security standards
- Ensuring regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party service Staying Put is considering using to store or process data

The Digital Communications Manager is responsible for:

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines:

- The only people able to access data covered by this policy should be those who need it for their work
- Data is not to be shared informally. When access to confidential information is required, employees can request it from their line managers
- All Staying Put employees are required to attend annual training to help them understand their responsibilities when handling data
- Employees are to keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords alongside two factor authentication must be used and they should never be shared
- Personal data is not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated. If no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection

**2. Data Storage:**

- When data is stored on paper, it should be kept in a secure place such as a locked drawer or filing cabinet when not being used, where unauthorised people cannot see it
- Data printouts should be shredded and disposed of securely when no longer required
- All electronic data must be protected from unauthorised access, accidental deletion and malicious hacking
- Data should only be stored on removable media (for example USB), with the permission of line management and these should be kept securely when not in use. The IT and Business Support Lead will provide the removable media
- Data is only to be stored on designated drives and servers, and should only be uploaded to approved company cloud computing services
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data are to be protected by approved security software and a firewall

**3. Data Use:**

- When working with personal data, employees should ensure the screen of their computers/tablets are always locked when left unattended.
- Personal data should be not shared informally. It should never be sent by email (unless it's a secure or encrypted email address) as this form of communication is not secure.
- Employees should not save copies of personal data to their own computers.

**4. Data accuracy:**

- The law requires Staying Put to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees to take reasonable steps to ensure data is accurate and up to date.
- Data will be held in as few places as necessary. Staff are not to create any unnecessary additional data sets.
- Staff are to take every opportunity to ensure data is updated. For instance, by confirming client details when they call and updating any inaccuracies/changes on OASIS.

**5. Confidential Information**

**5.1 Information about service users**

Information on service users will be shared on a need-to-know basis. Personal details disclosed by an individual on a one-to-one basis will remain confidential unless the following circumstances prevail:

- There is a direct effect on the safety of the individuals

- There is a child protection concern
- A service user is threatening to self-harm, or end their life

A service user's permission will be obtained before disclosing personal data to a third party (Appendix 1). The only time this will be overridden is if:

- There is a child protection concern
- There is a need to protect the vital interests of the service user (i.e. it is a life-or-death situation)
- Staying Put is required by law to do so
- Staying Put is assisting in the prevention or detection of a crime
- There is a Multi-Agency Risk Assessment Conference (MARAC)

Where external agencies have ongoing relationships with service users, all parties concerned will agree on boundaries of confidentiality.

Information about children and young people - in the event of any disclosure of child abuse, the Safeguarding Children policy and procedure must be followed.

Information about ex-service users - Confidentiality is just as important for ex-service users of Staying Put as it is for current service users accessing our services. This policy and procedure applies to ex-service users and their children.

**5.2 Staff, Volunteers and Board Members**

Under no circumstances will information relating to a staff member, volunteer or trustee be shared with any individual or organisation without the permission of that person.

The address of any of Staying Put's provisions will not be given out or discussed with anyone unless in exceptional circumstances. The likely exceptions are partner agencies attending professional meetings, professional agencies for business use only, and approved contractors including where legal requirements necessitate knowledge or direct access. Staying Put will attempt to minimise the number of people who know of its premises across the district by using the same contractors and dealing with the same person at an agency where possible. All staff; volunteers and trustees are required to agree and complete Appendix 2 during the induction to their role.

Staff responsible for employing contractors and consultants must explain Staying Put's expectations as regards confidentiality. They must also agree and sign the Confidentiality Contract for Contractors (Appendix 3).

Staff responsible for linking with partner agencies are responsible for informing them about Staying Put's Confidentiality Policy. Breaches of confidentiality by either party will be treated as a breach of the agreement. They must also agree and sign the Confidentiality Contract for Contractors (Appendix 3).

Under no circumstances should the work of Staying Put be discussed in a non-professional situation outside of the working environment. This includes general conversation with colleagues, friends, and family.

**6. Data Breaches**

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery, unless the breach is unlikely to result in a risk to the rights of data subjects. In addition, where legally required, we will also have to notify affected data subjects where the breach is likely to result in a "high risk" to their rights.

**7. Training**
New employees must read and understand the policies on confidentiality and data protection as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

All employees are sufficiently trained to protect individuals' personal data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

**8. Subject access requests:**
All individuals who are the subject of personal data held by Staying Put are entitled to:

- Ask what personal information the company hold about them
- Request access to their personal data held by us
- Ask to have inaccurate personal data rectified or deleted
- Be informed how to keep their information up to date
- Withdraw consent when we are relying on their consent for the processing
- Be informed how the company is meeting its data protection obligations
- Raise a complaint about the way their data is being processed

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests should be made in writing and addressed to the Executive Assistant, Staying Put, PO Box 449, Bradford, BD1 2XB, or by email to referrals@stayingput.org.uk

The data controller is required to provide the relevant data within 28 days. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.

The Executive Assistant, or Safeguarding Lead in their absence, will verify the identity of anyone making a subject request before handing over any information.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Staying Put will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Information Commissioners Office, the board and from the company's legal advisors where necessary.

**9. Data Retention**
Data will be retained as necessary and records will be retained for up to six years after the date that you leave our service in case legal proceedings arise during that period. Data will only be retained for a period of longer than six years if it is material to legal proceedings or should otherwise be retained in our interests after that period (Appendix 4)

## Amendment Log

| Date of revision: | Reason for revision: | Consultation record: | Record of amendments: |
|---|---|---|---|
| March 2024 | Merge of confidentiality and data protection policies | Policy Created | |
| September 2024 | Update | HR | Addition of the Caldicott Guardian |
| February 2026 | Document Review | Head of Operations & CC | Minor wording changes.<br>Inclusion of Executive Assistant in the SAR procedure<br>Minor wording changes to Appendix 4 |

| | |
|---|---|
| Date Agreed by Board | March 2024 |
| Next Review Date | February 2028 |

## Appendix 1 Staying Put - Client Consent Form

**Client Name …….** **Client ID:…….**

In keeping with our policy on confidentiality, it is necessary for us to obtain your permission to store, process and share data with appropriate third parties in line with GDPR regulations. In all cases, information will only be shared on a 'need to know' basis where it may help to ensure that your case progresses effectively.

Please circle those organisations, which you would be happy for us to liaise with on your behalf if necessary.

| **Agency** | | **Agency** | |
|---|---|---|---|
| Social Care | Yes / No | Victim Offender Unit | Yes / No |
| School/Education | Yes / No | Housing | Yes / No |
| Health Visitor | Yes / No | Benefits Agency | Yes / No |
| Health (GP/Consultant) | Yes / No | Refuge | Yes / No |
| Solicitors | Yes / No | Immigration | Yes / No |
| Police | Yes / No | Drug/Alcohol agency | Yes / No |
| Probation | Yes / No | Other (please specify) | |

In certain circumstances, it may be necessary for us to share information with other agencies even when you may not wish to give permission. These circumstances are as follows:

1. If we believe that withholding information may place either yourself or workers at significant risk if, for example:
    - There is a danger of assault
    - There is a serious risk to health
    - There is a serious risk from the environment
2. If we are concerned that your child/children are at risk of harm
3. Staying Put is required to do so by law
4. Staying Put is assisting in the prevention or detection of a crime

The decision makers in cases where we may need to breach confidentiality would be the keyworker and their Line Manager. Every effort would be made to discuss this with you and notify you of the decision before any action was taken.

Please sign below to confirm that this form has been fully explained to you and that you understand and agree to the above.

**Client's Signature……Date……**

## Appendix 2

**CONFIDENTIALITY CONTRACT – Staff, Service Users, Volunteers & Trustees**

In your dealings with Staying Put, you will have access to sensitive information and data concerning service users and their children. You will also have access to confidential information such as the location of Staying Put premises, partner premises, service user homes, refuges and hostels.

Information will be provided to you on a 'need to know' basis only.

To safeguard us all and the long term-viability of the organisation whether in a personal or professional capacity, the following applies, unless Staying Put gives their express permission to do so-

- The address of any of our premises must not be disclosed to any person, apart from a general indication of their location i.e. that it is situated in Bradford.
- No recorded or unrecorded data/information relating to the Business of Staying Put can be shared
- No recorded or unrecorded data/information about our service users, staff, volunteers or Trustees can be shared

An ongoing agreement and ability to honour the terms of this contract will be a requirement of your continued liaison with Staying Put.

**Acceptance of the terms of the confidentiality contract**

I have read and understood the above information. In working with Staying Put, I undertake to respect the confidentiality of the organisation, its business and people whilst involved with Staying Put now and in the future.

Name:

Signed:

Date:

## Appendix 3

**Confidentiality Agreement – Contractors & Other Agencies**

I……..of…….……agree (In line with mutual understanding between my organisation and Staying Put about the importance of confidentiality in the work of Staying Put)

1. To observe the strictest confidentiality regarding the addresses of the organisation.

2. Not to disclose the identity of any member of staff of Staying Put to anyone except where required to do so by a senior manager of my organisation acting properly in the course of my duties, or where obliged to do so by law.

3. Not to disclose any information relating to the nature of Staying Put's business as a domestic abuse and Sexual Violence support service

I understand that if my organisation discovers that I have breached these instructions-

a) That it will notify the Safeguarding Lead of Staying Put immediately to enable any precautions to be taken and it will consider taking appropriate action against me.

b) May lead to formal action with my current employer.

Signed…….

Name

Position in Organisation

Date

## Appendix 4 – Retention and Disposal Schedule

### 1. Management & Organisation

| Ref | Record | Minimum Retention Period | Action After Retention Period |
|---|---|---|---|
| 1.1 | Board of Trustees - Minutes general correspondence | 6 years from the date of meeting under the Charitable<br>Incorporated Organisations (general) Regulations 2012 | Destroy |
| 1.2 | Executive Group - Meeting Minutes | Recommendation: 6 years | Destroy |
| 1.3 | Staff Meeting Minutes | Recommendation: 6 years | Destroy |
| 1.4 | Policies | Recommendation: Retain while current. Retain 1 copy of old policy for 2 years after being replaced | Destroy |
| 1.5 | Comments/Complaints | Recommendation: 5 years after closing.<br>Review for further retention in the case of contentious disputes | Destroy |
| 1.6 | Annual Report | Recommendation: Retain for 10 years | Destroy |
| 1.7 | Emergency Planning/Business Continuity Plan | Recommendation: Until superseded | Destroy |

**2. Service Users**

| Ref | Record | Minimum Retention Period | Action After Retention Period |
|---|---|---|---|
| **2.1** | **Children** | | |
| 2.1a | Applications for services | 7 years from date of application to use the service | Destroy |
| 2.1b | Service user records | 7 years from termination of service to use the service under the Limitation Act 1980 as amended. ("Applications" includes direct applications to use a service by families or referrals from third parties) | Destroy |
| 2.1c | Child Protection Information – records of concern by the Charity where no referral has been made | Recommended: Until the child is 21 unless transferred onto adult services, in such instance 7 years from termination of service unless otherwise specified in the funding contract | Destroy |
| 2.1d | Child Protection Information – where a Child Protection Investigation or Serious Case Review has been undertaken by the Local Authority | Retain on file at least until the person reaches state pension age (NSPCC guidance) | Destroy |
| 2.1e | Records naming a child on the Child Protection Register | Retain on file at least until the person reaches state pension age (NSPCC guidance) | Destroy |
| 2.1f | Records of concern in relation to potential historic child abuse allegations | Retain on file at least until the person reaches state pension age (NSPCC guidance) | Destroy |
| 2.1g | Records of safeguarding referrals | Retain on file at least until the person reaches state pension age (NSPCC guidance) | Destroy |

| | | | |
|---|---|---|---|
| 2.1h | Records relating to mental health support | Recommended: 20 years after the date of last contact or 8 years after death, whichever is the sooner (NHS guidance) | Destroy |
| 2.1i | Deputy and trustee services | Retain on file for 100 years from termination of service.<br>Under the Limitations Act 1980 there is no time limit for | Destroy |
| **2.2** | **Adults** | | |
| 2.2a | Applications for services | 7 years from date of application | Destroy |
| 2.2b | Service user records | Recommended: 7 years from termination of service unless otherwise specified in the funding contract | Destroy |
| 2.2c | Child Protection – records of allegations or referrals including where the Local Authority have completed a serious case investigation | Retain on file at least until the person reaches state pension age under NSPCC guidance | Destroy |
| 2.2d | Records of safeguarding referrals | Recommended: 7 years from termination of service unless otherwise specified in the funding contract | Destroy |
| 2.2e | Records of concern in relation to potential historic child abuse allegations | Recommended: Retain on file at least until the person reaches state pension age (NSPCC guidance) | Destroy |
| 2.2f | Records relating to mental health support | Recommended: 20 years after the date of last contact or 8 years after death, whichever is the sooner under NHS guidance | Destroy |

| | | | |
|---|---|---|---|
| 2.2h | Deputy and trustee services | Retain on file for 100 years from termination of service. Under the Limitations Act 1980 there is no time limit for claims on trust property where a trustee has acted fraudulently or retained proceeds owed to the trustee. | Destroy |

**3. Staff**

| Ref | Record | Minimum Retention Period | Action After Retention Period |
|---|---|---|---|
| 3.1 | Interview notes and recruitment records | Date of interview + 6 months (ICO guidance) | Destroy |
| 3.2 | Right to work checks | 2 years after leaving employment (Home Office Requirements) | Destroy |
| 3.3 | Staff Personnel Records (including, appointment details, training, staff development etc.) | Recommendation: 7 years after leaving employment | Destroy |
| 3.4 | Staff Salary Records | 7 years after leaving employment (required by the Taxes Management Act 1970) | Destroy |
| 3.5 | Staff PAYE Records | 3 years after the end of the tax year to which they relate (required by the Income Tax (Pay As You Earn) Regulations 2003) | Destroy |
| 3.6 | Staff Sickness Records (copies of Medical Certs) | Recommendation: 3 years after the end of the tax year to which they relate | Destroy |
| 3.7 | Staff Maternity and Paternity pay records | 3 years after the end of the tax year in which the maternity period ends (required by the Statutory Maternity Pay (General) Regulations 1986) | Destroy |

| | | | |
|---|---|---|---|
| 3.8 | Staff Performance Review | Recommendation: 7 years after leaving employment | Destroy |
| 3.9 | Procedures for Induction of Staff | Recommendation: Until superseded | Destroy |
| 3.10 | Volunteer Personnel Records | Recommendation: 7 years after last known date of active service. DBS checks to be destroyed after 6 months of leaving | Destroy |
| 3.11 | Self-employed Specialist Records | Recommendation: 7 years after last known date of active service | Destroy |
| 3.12 | Disclosure and Barring Checks | Recommended: 6 months after leaving subject to the DBS Code of Practice (NSPCC guidance). | DBS Code of Practice: Retain the following after certificate is destroyed:<br>• the date of issue of a Disclosure<br>• the name of the subject<br>• the type of Disclosure requested |

**4. Finance**

| Ref | Record | Minimum Retention Period | Action After Retention Period |
|---|---|---|---|
| 4.1 | Annual budget and budget deployment | Recommendation: 7 years | Retain electronically on ExpensePlus / Sharepoint |
| 4.2 | Budget monitoring | Recommendation: 7 years | Retain electronically on Sharepoint |
| 4.3 | Management accounts | Recommendation: 7 years | Retain electronically on Sharepoint |
| 4.4 | Invoices | Recommendation: 7 years | Retain electronically on ExpensePlus |

| | | | |
|---|---|---|---|
| 4.5 | Bank statements | Recommendation: 7 years | Retain electronically on Sharepoint |
| 4.5 | Audit Reports | Recommendation: 7 years | Retain electronically on Sharepoint |

**5. Health & Safety**

| Ref | Record | Minimum Retention Period | Action After Retention Period |
|---|---|---|---|
| 5.1 | Accident Reporting | 3 years after the date of the incident (required by the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013)<br><br>Recommended: Date of incident + 7 years | Destroy |
| 5.2 | Risk Assessments | Recommendation: 3 years (per Moorepay guidance) | Destroy |
| 5.3 | Insurance liability documents | Recommendation: 40 years from date of issue unless contract states otherwise (Health and Safety Executive recommendation) | Destroy |
| 5.4 | H & S Reports | Recommendation: 5 years (per Moorepay guidance) | Destroy |
| 5.5 | Fire Procedure | Recommendation: Until superseded | Destroy |
| 5.6 | Security System File | Recommendation: For the life of the system | Destroy |

In scenarios where legal action is threatened or imminent the above dates of destruction may on a case-by-case basis be considered and extended for no longer than is reasonable for the completion of any such legal action and cooperation with any legal duties of disclosure on the Charity.